CLAIMS

1. A method for encrypted communications between a first transceiver and a second transceiver, the method comprising:

sending from a first transceiver to a second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets.

2. The method of claim 1, wherein the exchange threshold is a time.

3. The method of claim 1, wherein the exchange threshold is a counter value.

4. The method of claim 1, wherein the exchange threshold is a number of packets.

5. The method of claim 1, wherein the exchange threshold is at least one of a time, a counter value, and a number of packets.

6. The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a session is to be at least one of aborted or retried when the timeout limit is satisfied.

7. The method of claim 1, wherein the request to initiate derivation of the new encryption key is sent from the first transceiver to the second transceiver and the new encryption key is to be generated at the second transceiver, in response to the

request, before a key space of an old nonce value has been exhausted.

8. The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key.

9. The method of claim 8, further comprising:
sending from a second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce needed to derive the new encryption key.

10. The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a first transceiver authentication indication that authenticates the first transceiver to the second transceiver.

11. The method of claim 10, further comprising sending from the second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second transceiver authentication indication which authenticates the second transceiver to the first transceiver.

12. The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value that is used along with the new encryption key for encryption.

13. The method of claim 12, further comprising:
sending from a second transceiver, in response to the request to initiate derivation of the new encryption key, a

status indication indicative of the second transceiver's determination of the feasibility of being able to commence using the new encryption key at the second transceiver in accordance with the exchange threshold.

14. The method of claim 1, further comprising:

determining whether the new encryption key needs to be derived; and

wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived.

15. The method of claim 1, further comprising:

generating the new encryption key at the first transceiver and the second transceiver;

determining at at least one of the first transceiver and the second transceiver whether the exchange threshold has been satisfied; and

encrypting at at least one of the first transceiver and the second transceiver using the new encryption key when the exchange threshold has been satisfied.

16. The method of claim 15 further comprising:

continuing communication between the first transceiver and the second transceiver using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.

17. The method of claim 16 wherein encrypting using the new encryption key occurs without disrupting communication between the first transceiver and the second transceiver.

18. The method of claim 1, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key, the method further comprising:

sending from a second transceiver to the first transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce needed to derive the new encryption key.

19. The method of claim 18, further comprising:

generating at at least one of the first transceiver and the second transceiver the new encryption key;

determining at at least one of the first transceiver and the second transceiver whether the exchange threshold has been satisfied; and

encrypting at at least one of the first transceiver and the second transceiver using the new encryption key when the exchange threshold has been satisfied.

20. The method of claim 19, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value and encrypting includes using the initial nonce value and the new encryption key for encryption, the method further comprising:

determining whether the new encryption key needs to be derived; and

wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived.

21. The method of claim 20, the method comprising:

sending from first receiver to the second transceiver a first transceiver authentication indication that authenticates the first transceiver to the second transceiver; and

sending from the second transceiver to the first transceiver a second transceiver authentication indication that authenticates the second transceiver to the first transceiver.

22. The method of claim 21, further comprising sending from the first transceiver to the second transceiver the second nonce.

23. The method of claim 22 further comprising:

continuing communication between the first transceiver and the second transceiver using an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.

24. The method of claim 23 wherein encrypting using the new encryption key occurs without disrupting communication between the first transceiver and the second transceiver.

25. The method of claim 24, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a communication is one of aborted and retried when the timeout limit is satisfied.

26. A first transceiver that is to conduct encrypted communications with a second transceiver, the first transceiver comprising:

a physical control layer that sends to the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange

threshold indicative of when the new encryption key is to be used to encrypt communication packets.

27. The first transceiver of claim 23, wherein the exchange threshold is a number of packets.

28. The first transceiver of claim 23, wherein the request includes a first transceiver identifier that authenticates the first transceiver to the second transceiver.

29. The first transceiver of claim 23, wherein the request to initiate derivation of the new encryption key includes a timeout limit that indicates that a session is to be at least one of aborted or retried when the timeout limit is satisfied.

30. The first transceiver of claim 23, wherein the request to initiate derivation of the new encryption key includes a first nonce needed to derive the new encryption key.

31. The first transceiver of claim 23, wherein the request to initiate derivation of the new encryption key includes a first transceiver authentication indication that authenticates the first transceiver to the second transceiver.

32. The first transceiver of claim 23, wherein the request to initiate derivation of the new encryption key includes a new initial nonce value that is used in combination with the new encryption key for encryption.

33. The first transceiver of claim 23, wherein the physical control layer determines whether the new encryption key needs to

be derived before sending the request to initiate derivation of the new encryption key; and

wherein sending the request to initiate derivation of the new encryption key is based upon the determination of whether the new encryption key needs to be derived.

34. The first transceiver of claim 23, wherein the physical layer receives a second nonce from the second transceiver, generates the new encryption key, determines whether the exchange threshold has been satisfied, and encrypts using the new encryption key when the exchange threshold has been satisfied.

35. The first transceiver of claim 34 wherein the physical control layer continues using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.

36. The first transceiver of claim 23, wherein the physical control layer sends the request early enough so that the new encryption key is to be generated at the second transceiver, in response to the request, before a key space of an old nonce value has been exhausted.

37. A first transceiver that is to conduct encrypted communications with a second transceiver, the first transceiver comprising:

a physical control layer that receives from the second transceiver a request to initiate derivation of a new encryption key, the request to initiate a new encryption key derivation being controlled by a MAC sub-layer and including an exchange threshold indicative of when the new encryption key is to be used

to encrypt communication packets, and a first nonce needed to derive the new encryption key.

38. The first transceiver of claim 37, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a second nonce.

39. The first transceiver of claim 37, wherein the physical control layer sends to the second transceiver, in response to the request to initiate derivation of the new encryption key, a status indication indicative of the first transceiver's determination of the feasibility of being able to commence using the new encryption key at the first transceiver in accordance with the exchange threshold.

40. The first transceiver of claim 37, wherein the physical control layer generates the new encryption key determines whether the exchange threshold has been satisfied, and encrypts using the new encryption key when the exchange threshold has been satisfied.

41. The first transceiver of claim 39 wherein the physical control layer continues communication between the first transceiver and the second transceiver using for encryption an old encryption key generated before the new encryption key when the exchange threshold has still not been satisfied.